21615518

DRAFT

RTD

SOUTHERN CALIFORNIA
RAPID TRANSIT DISTRICT

District Information Security Policy and Guidelines

MARCH 1989

SOUTHERN CALIFORNIA RAPID TRANSIT DISTRICT
INFORMATION SECURITY POLICY

Table of Contents

INFORMATION SECURITY POLICY

I. INTRODUCTION

The District's information resources and systems have become a critical business asset and information processing capability has become an indispensable resource. As such, the security, reliability and integrity of the associated data, processes, and systems are of vital importance to the continued operation of the District.

The District's information asset is defined as the information processing resources and capabilities required in the preparation and retention of information. Information assets may reside in many forms; magnetic storage media, computer hardware, printed material and purchased or developed software systems.

Information asset protection is defined as the measures and operations that are necessary to ensure that District information and resources are protected against unauthorized use, modification, dissemination, or destruction. The level of protection given to individual elements or collections of information shall be commensurate with the value to the District or the potential costs or risks associated with its misuse, whichever is higher.

II. PURPOSE

The purpose of this policy is to document senior District management commitments pertaining to the security and recoverability of District information processing resources and operations and to identify high-level items of policy that support the commitments.

III. SECURITY POLICY STATEMENT

It is RTD's management general policy to observe sound security practices, uphold contractual obligations, and comply with regulatory requirements regarding information protection as well as all applicable laws including statutes addressing:

- Copyright matters
- Trade Secret protection, and;
- Computer Crime

Any violation of law related to information processing involving District information assets by employees or contractors is a violation of this District Information Security Policy, and may result in disciplinary action and/or civil or criminal prosecution.

IV. SCOPE OF POLICY

This policy shall apply to all information maintained and created within the District's information systems. This includes, but is not limited to information created and maintained within:

1. The District's central data processing department,
2. Decentralized District mini or micro computer systems,
3. Any remote District processing centers,
4. Any District department or contract user of data processing resources, commonly through remote terminals, and/or;
5. Any services organization which processes data for the District.

V. GENERAL RESPONSIBILITIES

A. INFORMATION SECURITY

1. The Management Information Systems Department information security function will be responsible for performing ongoing administration of security systems as defined by the "Information Security Functional Charter".

B. DISTRICT MANAGEMENT

The District's management team is ultimately responsible for securing information in accordance with Information Security Guidelines.

1. Each Manager must assess information they use in the day to day conduct of business and estimate:

   a. The value of the data to the District.
   b. The costs and implications of misuse of data.

2. Based on their assessment, management must determine the appropriate level of protection in accordance with Information Security guidelines.

C. PERSONNEL AND USERS

It is the responsibility of all District personnel to read, sign an acknowledgement of and comply with an extract of policies from this document (pertaining to general restriction of access to and usage of information processing resources), and to immediately report any known or suspected violations of the policies cited to Information Security.

It is the responsibility of all users of District information processing resources to read, sign an acknowledgement of and comply with all provisions of this document, and to immediately report any known or suspected violations of any policy contained herein to Information Security.

VI. DISTRICT COMMITMENTS

1. The District recognizes that its many information processing resources and operations present security and recovery issues that have the potential to impact District-wide operations. The District further recognizes that to adequately address these issues on a District-wide scale, a comprehensive, uniform and consistent program of information security is required, and that any such program must operate on a foundation of centralized policies, overview and control for it to be effective.

   On the basis of this recognition, the District is committed to the development and support of a centralized information security function, known as "Information Security". Information Security shall have the duty, authority and responsibility to protect District information processing resources and operations through:

   a. Identification and reporting of relevant risks, exposures, threats and incidents,

   b. Development of relevant security measures, policies, procedures, standards and guidelines for management approval,

   c. Implementation and enforcement of security measures, policies, procedures, standards and guidelines adopted by management, and;

   d. Appropriate intervention into information security incidents or emergencies.

   The Information Security function shall be headed by an individual designated as the Information Security Officer. Security controls shall be centralized under the function to the extent necessary to ensure the security and recoverability of District information processing resources and capabilities. The District shall adopt and maintain a detailed functional charter that defines the mission and scope of operations of Information Security, and provides sufficient autonomy and authority for the function to operate effectively and with integrity.

   Information Security shall be empowered with unrestricted access to information processing resources and sufficient authority to act upon such resources to enable it to perform both proactive and reactive security and recovery operations without dependency upon other functions. Reactive authority includes charter to respond to security incidents or other emergencies with direct intervention as well as preventative control measures.

All functional activities of Information Security shall remain fully accountable to its chain of command at all times, and are subject to examination or audit by the Office of the Inspector General at any time.

2. District management shall support viable security measures for information processing resources and capabilities, extending protection from injury, damage or loss to personnel, data processing equipment, facilities, data, programs, libraries and related documentation, as appropriate. This protection will include (as applicable), protection from unauthorized access, use, disclosure, transfer, alteration, modification or destruction. Assumption of risk shall not be standard practice.

3. The District shall maintain information processing disaster recovery capability including arrangements for recovery operations facilities, ongoing maintenance and testing of a comprehensive contingency plan and the ongoing operations of a comprehensive vital record backup and protection routine.

4. The District shall use its best efforts to prevent the use of its information processing resources and capabilities to violate any law, regulatory requirement, civil responsibility or contractual obligation, to include protection of the privacy or proprietary rights of employees, contractors, and organizations with which it has conducted business.

5. Information Security will develop specific, written policies, procedures, standards and guidelines as necessary to reinforce and uphold items of policy set out in this document. Upon approval of management, these supporting elements of policy will become extensions of this document for all intents and purposes. At that time, Information Security will be responsible for dissemination of relevant information through appropriate announcements, training and awareness effort, as well as the ongoing enforcement of all such supplemental security policies.

6. The District shall levy disciplinary action such as formal reprimand, suspension or termination against any District employee who willfully or negligently violates District Information Security Policy. When deemed appropriate, the District will bring civil action against and/or pursue criminal

prosecution of District employees or non-employees who violate legally-protected interests of the District and/or any criminal law, as applicable to information security issues.

7. The District shall maintain its information security program as a measure of excellence, comparable to customer service, efficiency or public accountability.

VII. INFORMATION SECURITY POINTS OF POLICY

1. The use of information processing resources, including hardware, software storage media, personnel services, computer supplies and computer system time shall be restricted to support of District business activities. Because no personal use of District assets is permitted, there shall be no expectation of privacy by any person regarding their utilization of information processing resources belonging to or used by the District.

2. The District shall use its best efforts to conduct its information processing operations in a manner that will ensure individual accountability for all data, transactions, commands and communications entered into its computer systems. Wherever technically feasible, no single user access control and/or identification shall be used by more than one individual.

3. All users of District systems shall be personally accountable for data, transactions, commands and communications entered or derived through the use of their assigned computer system identification, password, access code or physical security mechanism, or by any other means under their control. System users are individually responsible for safeguarding any such means of access to computers assigned to them, and for the immediate reporting of the loss or compromise of such controls to Information Security.

4. Physical access to information processing resources shall be restricted to authorized personnel as designated by the management staff having custody and control of the resources. Such access will be based solely upon the functional necessities of the District, and may be limited as to the place, time and extent of access and/or subject to other conditions that may be deemed to be appropriate. No access shall be authorized as a privilege or token of position.

5. "Perimeter security" for computers utilized by the District shall be maintained at all times through sound security practices, including periodic password changes, adherence to password composition guidelines and immediate notification of Information Security of the transfer or termination of any computer user. Such notifications are the responsibility of the immediate supervisor of the affected computer user and/or the District staff member who initially authorized the user's access.

6. All data stored or utilized on computers used by the District shall be under the care and control of designated "conservators", who are responsible and accountable for authorization of access to and usage of all data placed in their care. Such authorizations will be based solely upon the functional necessities of the District, and may be limited as to the place, time and extent of access and/or subject to other conditions that may be deemed to be appropriate. No access shall be authorized as a privilege or token of position.

7. Guidelines shall be maintained to classify all District data resources (regardless of form or media of presentation) on the basis of value and sensitivity into distinctive, separate categories. Appropriate security requirements will be defined for each category, governing the generation, storage, usage and disposal of information according to its classification.

   "Conservators" and "custodians" of information resources shall be responsible and accountable for self-assessment, classification and marking of information resources in their care and for maintenance of required levels of accountability and control over such resources, in accordance with the security requirements defined for each classification.

8. "Production" programs and data shall remain segregated from development or test programs and data. To the greatest extent possible, no information processing will be permitted that would apply development or test resources to update, modify, add or delete "production" resources. Exceptions will be subject to strict change controls and quality assurance measures.

9. The availability of programs or utilities having the capability to circumvent computer security mechanisms or to do great harm to information processing resources or operations will be restricted to the absolute minimum number of individuals necessary to meet the needs of the District's technical functions. The levels of responsibility towards security issues and technical competence demonstrated by personnel either

requesting or holding access to such programs or utilities shall be the primary and overriding consideration during initial and ongoing authorization of such access. No access shall be authorized as a privilege or token of position.

10. The District shall not undertake any new computer applications or operations, or initiate changes thereto, unless adequate security and recoverability have been reasonably assured. Acquisition, modification or development of computer facilities, hardware, software, firmware or applications must conform to all applicable District Information Security Policy items, and is subject to further review for compliance with supplemental policies, standards and guidelines by Information Security.

11. Any centralized, distributed or stand-alone information processing operation or resource shall be subject to regulatory control by the Management Information Systems (MIS) Department, if it has one or more of the following characteristics:

    a. Constitutes an operational dependency for any District function,

    b. Feeds or directly affects a District computer application supported by the Management Information Systems (MIS) Department,

    c. Crosses departmental lines and/or has the potential to directly affect operations in any District department other than the host department,

    d. Presents resource management or performance issues affecting the operations of MIS-based systems,

    e. Utilizes "production" data resources (other than via MIS-based computer applications), or;

    f. Utilizes mainframe computer programming languages such as COBOL, FORTRAN or ASSEMBLER, with the exception of certain fourth-generation languages such as FOCUS, ANSWER DB, HIGHLIGHT, SPSS or IMAGINE (all exceptions being subject to MIS approval).

12. The District's Management Information Systems Department shall maintain viable separation of duties among its application programming, systems programming, computer operations, data entry and information security functions.

13. It shall be the responsibility of all District employees to protect District information resources under their custody or control, not only through compliance with established District and Information Security policies, but also in accordance with reasonable care and the basic duty of loyalty to an employer. This responsibility includes the duty to immediately report all known or suspected actual or attempted information security violations, breaches or incidents to Information Security.

    It is the further responsibility of each District employee to initiate any and all inquiries that may be necessary to ensure the employee's complete understanding of and compliance with information security policies, procedures, standards and guidelines. All such inquiries should be directed through the employee's chain of command or to Information Security.

14. Any actual or attempted compromise, intrusion upon or interference with the duties or operations of the Information Security function by anyone external to the Information Security chain of command shall constitute either a security breach or security incident, and will be addressed appropriately, except in any instance wherein a prohibited action results from a due process of law.

VIII. DEFINITIONS

Data Conservator - is defined as a division manager or representative that specifies data control requirements to data custodians and users of this data.

Data Custodian - is defined as a provider of services in support of the District's internal business operation.

Data User - is defined as anyone who accesses, uses, or retains District data.

Perimeter Security - The first line of defense in security controls over District systems, consisting of all system and application security directories that control initial access to any idle terminal. This perimeter forms the boundary between District systems and unauthorized users, including former employees and the rest of the outside world. Unless effective security is maintained throughout this perimeter, all internal security is subject to compromise because an intruder can assume the identity of an authorized user.

Production - Any form of centralized, distributed or stand-alone information processing operation or resource having one or more of the following characteristics:

a. Constitutes an operational dependency for any District function,

b. Feeds or directly affects a District computer application supported by the Management Information Systems (MIS) Department, or;

c. Crosses departmental lines and/or has the potential to directly affect operations in any District department other than the host department.

IX. ADEQUACY STANDARD

This policy, and all supporting standards, procedures, and guidelines issued in support of the policy shall serve as an adequacy standard for information security standards; i.e., the basis on which audits will be conducted.

X. ENFORCEMENT

The Information Security function will enforce standards, procedures or guidelines established pursuant to this policy and report violations to management for appropriate action.

SOUTHERN CALIFORNIA RAPID TRANSIT DISTRICT
INFORMATION SYSTEMS SECURITY GUIDELINES
TABLE OF CONTENTS

Page

I. RESPONSIBILITIES AND REQUIREMENTS

A. BASIC RESPONSIBILITIES

1. **District Management.** District managers are responsible for:

   - Determination of ownership authority and responsibility for all of the District's information assets;
   - Awareness of Information Security for resources for which they are responsible and applicable control requirements;
   - Authorizing users to utilize computer systems and data under their guardianship;
   - Assigning custodian authority and responsibility;
   - Ensuring effective use of control facilities;
   - Their employee's education and awareness;
   - Timely, effective response to identified audit issues, information asset protection exposures, and reported violations, breaches, and incidents;
   - Self assessment and input to security planning.

2. **Conservator.** A conservator is the Division manager or management representative who is responsible for making and communicating judgments and decisions on behalf of the District with regard to identification, classification, and protection of the District's information assets.

   The conservatorship conveys authority and responsibility for:

   - Judging the asset's value and importance to the District;
   - Classifying the asset and applying the specified protection controls. Responsibility may not be delegated;
   - Authorizing access and assigning custody;
   - Referring suppliers of services and users to existing control and protection requirements.
   - Periodically reviewing control and classification decisions;
   - Monitoring compliance.

3. **Data Custodians.** The Data Custodian is a provider of services to others or to themselves in support of the District's internal business operations, and could be vendors or service providers.

   Data Custodians are responsible for:

   - Complying with applicable directives, agreements, and District Security Policy;

   - Administering conservator specified business and asset protection controls for information assets in their custody;

   - Upholding or maintaining established provisions for access to classified information.

4. **Data User.** A Data User is an individual authorized to utilize information assets.

   Users of data processing services and facilities are responsible for:

   - Compliance with applicable information asset protection practices and directives and assets protection requirements.

5. **Inspector General (IG) EDP Auditor.** The responsibility of IG EDP audit will be as follows:

   - Perform EDP audits at each information processing location;

   - Perform application reviews of existing systems to ensure controls are in accordance with Information Security Policy.

   - Ensure that new systems have been designed in ~~new systems in~~ accordance with Information Security Policy.

   - Review and confirm adherence to:

     - MIS Department Standards and Procedures

     - Information Security Policy and Guidelines

     - Generally acceptable data processing management principles. (Computer Schedules, Systems Development progress reporting and other management tools should be used.);

- Point out areas where standards are needed;

- Advise the appropriate people on the findings of the EDP audit;

- Ensure that controls are not compromised by changes made to the system.

B. PROCEDURAL REQUIREMENTS

1. **Self Assessment and Planning.** Self assessments of information asset protection status must be conducted at least annually by conservator, user, and custodian management.

   In performing self assessments, management must:

   - Review information asset protection responsibility assignments;

   - Review and validate classifications of software and data;

   - Identify all information asset protection exposures;

   - Conduct risk assessments for all newly-identified exposures;

   - Revalidate existing compliance plans and risk acceptances.

   The end product of self assessment will be a committed information asset protection plan supported by a total accounting of identified exposures, the status of which is shown to be that of planned compliance within the current operating plan period or of risk acceptance.

2. **Risk Assessment and Risk Acceptance.** Risk assessment is the process of evaluating and documenting any identified non-compliance situation for the purpose of review by Information Security, which will, in turn, make recommendations to management on whether to establish a compliance plan or to accept the risk.

   Risk assessment may be initiated by conservators, users, or custodians.

   Risk acceptance is appropriate only when the risk assessment process has demonstrated that available options for achieving compliance have been identified and evaluated, and that compliance will have a significant and unacceptable business impact.

Risk acceptances must be documented, and maintained on file with Information Security.

3. **Satisfactory Compliance.** The installation of information asset protection controls and procedures, while giving the appearance of compliance, may not produce required results. Satisfactory compliance is achieved when controls are effectively used.

   Satisfactory compliance means:

   - Proper identification and classification of assets to be protected;
   - Consistency and continuity of control. In data processing applications, controls must be applied not only through software but also procedurally and physically where people are involved - for example, in job submission, control of volumes, and release of output;
   - Separation of functions so that collusion between two or more persons is required to avoid a control;
   - Timely detection and reporting of losses, discrepancies, security violations, breaches or incidents;
   - Timely, effective response to reports of losses and discrepancies;
   - Sufficient record keeping and personal accountability sufficient for after-the-fact investigation of loss or impropriety and for appropriate management response, including personnel actions and pursuit of legal remedies;
   - The attribute of auditability.

4. **Records Required for Auditability.** Auditability is fundamental to all requirements established by this instruction. An auditable application is one whose performance according to specifications and compliance with control requirements can be demonstrated to, or formally tested by, an independent reviewer.

   The following records must be generated and maintained to assist in the auditing process.

   - Access authorization records.

- Self assessment documents and information asset protection plans.

- Risk assessment and risk acceptance documents.

- Reports of Restricted access, key, and password disclosure, custody change, decontrol, and disposal.

- Control element and restricted utility procedures, lists, access activity reports, and change specifications.

- Restricted access area logs and/or reports.

C. INFORMATION PROTECTION AND CONTROL

1. **Levels of Protection for District Information.** The following levels of classification have been established for protection of District information. For definitions, examples, and details of handling requirements, see Data Resource Management Standard. (To be published)

   - RTD Confidential
   - Unclassified

2. **Determining Appropriate Levels of Protection.** Output, including reports, data, and software, containing substantially the same information content as the input must be assigned classifications applicable to the input. Output that is a substantial modification of the input information or a merger of multiple inputs must be classified and controlled on its own merits.

   When system software does not have classification display capability, it must be provided by any new application programs or significant enhancements to existing programs that provide terminal display output.

   - Readable Output. Classified readable output including microfiche output, must be marked with applicable classifications that can be read without enlargement. In addition, each frame of classified microfiche output must contain applicable classifications.

   - The conservator has access authority to RTD Confidential information, and must specify any additional access, including the authorization to modify, update or copy such information.

D. SPECIFIC REQUIREMENTS

1. Sensitive Programs, Control Elements, and Restricted Utilities.

a. Sensitive Programs

A Sensitive Program is an application program whose unauthorized modification, for fraudulent purposes, could result in serious misappropriation or loss of the District's physical or financial assets, other than data. The objective of Sensitive Program control is prevention and detection of unauthorized program modification, substitution, or execution.

Sensitive Programs will normally be associated with control, edit, or audit functions, or with creation of negotiable instruments.

b. Control Elements and Restricted Utilities

Control Elements are software and data performing or supporting control functions such as access control, logging, and violation detection. Examples are: the Data Security System data sets, the TSO UADS data set, password data sets, files or cipher keys, log files and associated data reduction programs, hash total programs, Security System user exits, and non-cancellable IDs.

Restricted Utilities are software that can be used to alter or avoid such control functions as access control, logging and violation detection.

c. Required Controls for Sensitive Programs, Control Elements, and Restricted Utilities

Control objectives are to prevent unauthorized use, reproduction, modification, or substitution of software control mechanisms; unauthorized avoidance of software controls; and unauthorized modification of control information.

In addition to normal business controls, management must assign responsibility for the following required protective measures.

- Sensitive Programs, Control Elements, Restricted Utilities, and their stewards and custodians must be identified and listed.

- Written procedures must describe the overall control strategy, emergency procedures, and provisions for protection and backup, including off-site storage.

- Software must be access controlled, as appropriate, for read, update, and/or execution.

- Access for update of production software must be approved by Production Control.

- Reproduction of authorized versions and introduction or use of unauthorized copies is not allowed.

d. Additional Controls for Sensitive Programs

Programmers performing development or maintenance duties must neither be custodians of the production versions nor be allowed access thereto.

e. Disposal of Residual Information.

Residual information is processable information remaining from prior use of fixed or movable media. Classified residual information in storage, on volumes, and on magnetic media must be erased or overwritten by the application program. If erasure is not supported by the application software, it must be done manually.

2. Password Generation and Control. Responsible management, i.e., terminating manager of transferring manager, must ensure that verification and information access passwords are changed upon termination of the business need of any individual to whom the passwords have been disclosed.

Provision must exist for non-display or blotting of verification and information access passwords.

a. Non-Cancellable IDs

Non-Cancellable IDs are LOGON IDs and associated passwords that allow bypassing of normal security access control criteria. Because of the potential for misuse or subversion, Non-cancellable IDs are permitted on a tightly controlled need-only basis.

b. Global Verification Passwords

A verification password is the password that must be entered when signing on to a system. Its purpose is to validate that the person who entered the user identification is the authorized individual. Once the user identification has been verified, further access to information must be based on this identification.

Installation and user management must ensure that passwords used to verify user or job identification are:

- Classified "RTD Confidential";
- Randomly selected, not obvious or trivial;
- At least seven numeric, six alphabetic, or five alphanumeric characters in length;
- Changed at least every month, and more frequently in accordance with the requirements of appropriate security practices.

c. Information Access Passwords

An information access password is used to protect data that is stored in the system by associating a unique password with a particular file or data set. This password is presented to the system following logon when access to data is requested.

Only the system does not provide control of access to data based on verified user identification use of information access passwords for access control following logon or job initiation is allowed. Risk acceptances must be used as appropriate.

Any information access password must comply with all password generation and protection standards.

Responsible management must ensure that information access passwords are changed at least every month in accordance with District Security Policy.

3. a. Equipment and Systems not under District Control.

Equipment that connects to any District computer (mainframe, micro) or terminals but is not on the District's premises and not under District management control must adhere to the following specific requirements:

- Business necessity must be certified by two levels of management;

- Confidential Disclosure Agreements and other appropriate contracts must be in effect;

- Equipment must be used only for approved purposes, and usage must be authorized and verified by District management.

- Equipment must be operated in accordance with applicable District safety, security, and data processing asset protection requirements;

- Classified information, including materials, passwords, telephone numbers of computer dial ports, and waste, must be protected in accordance with MIS Standards and all data processing asset protection requirements as defined in this Instruction;

- Necessity must be re-established annually and compliance verified;

- The following functions must have concurred: MIS Management, Legal, Human Resources, Information Security, and Inspector General Audit.

b. Messages and Text.

District sending, forwarding, and receiving stations are subject to all information asset protection requirements, including marking messages and text with applicable security classifications.

II. <u>ROLE OF THE CONSERVATOR</u>

A. GENERAL REQUIREMENTS

1. Conservators must ensure that authorization to access information is current and that the authorization is deactivated upon termination of the user's business need.

2. Appropriate business controls must be implemented in all data processing applications. Business control considerations require that update authority for software and data be controlled and normally restricted to small populations of identified users. Similar restrictions of read and/or execute authority may be required in some cases.

3. Following logon or job initiation, logical access to transactions, software, and data must be controlled on the basis of previously validated user identification. (RACF is a control mechanism operating in this fashion.) When access to information and transactions cannot be controlled in this manner, alternatives such as information access password protection or encryption must be used. For small, stand-alone systems, physical access controls and administrative procedures must be employed to control logical access.

4. The conservator is not directly accountable for non-compliance by a custodian or a user. However, the conservator is expected to take reasonable steps to understand conditions surrounding the custody or use of the asset, to initiate appropriate actions when problems are identified, and to participate in the risk assessment process and risk acceptance decisions.

5. The conservator's authority to monitor compliance may be delegated, but compliance responsibility is not transferable.

B. APPLICATION DESIGN, DEVELOPMENT, AND IMPLEMENTATION

1. Application in this context refers to the end use of data processing services and facilities. The scope of an application extends to: data processing services used or invoked, application programs and associated software, input, output, data, procedures, documentation, and responsibility assignments.

2. All internal applications under development or significant enhancement, regardless of environment, must be reviewed for compliance with applicable District security policies and approved before becoming operational.

3. Operational applications must also be reviewed for compliance with District Security Policy during self assessment. Conservators must:

   - Identify assets and acknowledge conservatorship;

   - Classify input, output, data, and software for restrictive access;

   - Designate Sensitive Programs, Control Elements, and Restricted Utilities;

   - Specify and approve business controls;

- Specify and approve asset protection controls;
- Communicate controls to all affected parties;
- Monitor compliance with applicable controls;
- Review classification and controls for currentness and adequacy at least annually.

4. Conservators of common applications are responsible for the adequate documentation and communication of approved business and data processing asset protection controls to all users and custodians. Monitoring for compliance may require special attention and must be documented in a security plan.

5. Each form of software (source programs, object modules, procedures, etc.) must be separately classified and controlled on its own merits. For example, related source and load modules may be classified and controlled differently.

6. Information classified as sensitive or Confidential must not be used for software testing, except under specifically authorized and supervised conditions, such as final testing for newly developed or updated software.

7. All data and software must be associated with the conservator's identity, specified classifications and controls, and authorization lists as applicable.

8. Following logon or job initiation, control of logical access to software and data classified as sensitive or Confidential must take into account all possibilities: read, update (including deletion), and execution.

C. REQUIRED FUNCTIONS IN NEW APPLICATIONS. The following capabilities must be specified by conservators having applications developed if the capabilities are not in the control program:

1. Application access, including terminal logon and job initiation, must be controlled on the basis of verified user identification and authorization.

2. Access to software or data must be controlled on the basis of verified user identification and authorization.

3. When authorizations are not provided, access to software or data must be restricted to the conservator.

4. To forestall unauthorized access, repetitive attempts to gain access must be restricted.

5. Provision must exist for the non-display or blotting of classified passwords and keys.

6. Control of logical access to sensitive transactions, software, and data must be based on verified user identification. (RACF is a control mechanism operating in this fashion.)

7. Control of logical access to software and data must consider all possibilities: read, update, delete, and execute. Controls such as field within record, record within data base, and read-only and execute-only access must be specified and implemented when applicable.

8. Sensitive information must not be accepted from or released to terminals deviating from the control requirements of systems and sub-systems not under District control.

9. The ability must be present to erase residual information from storage, memory, and magnetic media.

III. ROLE OF THE CUSTODIAN

A. GENERAL REQUIREMENTS

1. Custodians of application systems and production data within a data processing facility must provide physical and procedural safeguards and must administer, or provide for the administration of, access to information as prescribed by conservators or as required by this Instruction or other directives.

2. Custodians may accept delegation of authority to grant access to information but may not directly grant access.

3. When compliance with required controls cannot be achieved without causing an unacceptable business impact, the custodian must initiate the necessary risk assessment and risk acceptance procedures.

4. Provision must be made for timely detection, reporting, and analysis of unauthorized attempts to gain computer, software, or data access. Responsibility for timely reaction to violations must be clearly assigned.

B. COMPUTING INSTALLATIONS AND SUPPORTING FACILITIES

1. Definitions

A computing installation is one or more computers used in the conduct of District business. Minicomputers or personal computers constitute a computing installation.

Supporting facilities are facilities supporting computing installations. Examples include: data entry areas, tape/disk libraries, terminal rooms or other input/output areas, printing installations, bursting/collating rooms, and power supply areas.

Use of the District's data processing services and facilities must be authorized by District management and, when applicable, controlled on the basis of verified user identification.

Custodians must effectively instruct application owners, information conservators, and users on available control facilities, required and recommended practices, and installation restrictions.

2. Physical Access Control

Computing installations and supporting facilities must be administered as areas of restricted physical access when continued operation is considered vital.

Measures must be implemented to prevent and detect attempts to disrupt operations or to enter or depart from restricted areas in an unauthorized manner.

Routine entry (i.e., logging and no escort or visual surveillance) must be allowed only to persons whose primary work stations are within the area.

Supporting telecommunication facilities such as telephone closets, wire rooms, and frame rooms must be administered as areas of restricted physical access.

3. Visitor Control

Each person in the installation must wear some readily visible identification indicating access authorization and whether the person is a visitor or a District employee.

Each entry and exit by persons whose primary work station is not within the areas must be logged. Reports of visitor and non-routine entry activity must be reviewed by management at least weekly. Responsibility must be clearly assigned for timely follow-up.

In order to prevent unauthorized access to information and to prevent unauthorized removal of information from the restricted access area:

- Authorized users such as programmers and authorized vendor service personnel and telephone company personnel must be kept under visual observation.

- All other visitors must be escorted.

Responsibility must be assigned to ensure that authorization documents are reviewed and authorizations are kept current.

4. System and Information Access Control

All data processing applications, software, and data must be identified with a conservator.

Computer access, including terminal logon and job initiation, must be controlled on the basis of verified user identification and authorization.

Authorization to use the District's data processing facilities and services and to access sensitive information must be current and deactivated upon notice of termination of the user's business need.

User identification codes must be traceable to the user for the lifetime of the records and reports in which they appear.

Custodians must be able to change or deactivate any computer access authorization at any time. In addition, the user must be provided some means for deactivating his access authorization or changing his access code in the event of known or suspected compromise.

Custodians must provide functions to:

- Control logical access to transactions, software, and data of verified user identification. (RACF is a control mechanism operating in this fashion.) When access to information and transactions cannot be controlled in this manner, alternatives such as information access password protection or encryption must be used.

- Custodians must classify telephone numbers of computer dial ports and control them accordingly. These telephone numbers must not be published in telephone directories or publicly posted.

C. CONTROL OF INFORMATION STORAGE MEDIA

1. Storage media is any mountable or demountable storage device such as a disk volumn, mass storage system cartridge, or magnetic tape reel or cartridge. In this Instruction, diskettes, cassettes, mag cards, and other small system media are considered to be magnetic input/output, but should be controlled as volumes.

2. Storage media must be controlled based upon the sensitivity of the information it contains and, whenever possible, marked accordingly.

D. TERMINALS

Custodians are responsible for ensuring that all terminals connected to the District computers for the purpose of conducting internal District business are under District control.

IV. ROLE OF THE USER

A. GENERAL REQUIREMENTS

1. Users of information data processing assets are responsible for compliance with security requirements and for compliance with control requirements specified by stewards and by custodians.

2. Data processing output is owned by the requesting user, unless other arrangements are made. Users who generate passwords are the owners of the passwords.

3. User management must ensure that stewards of District information or custodians, as appropriate, are notified upon termination of the user's business need for use of the information, services, or facilities.

B. APPLICATION ACCESS CONTROLS. The following access control requirements apply to users.

1. Verification passwords and user identifiers that serve as verification passwords must not be shared, and they must be: deactivated in event of known or suspected compromise, and the custodian notified.

2. Application function access passwords and cipher keys used as information access passwords must be:

   - Assigned the classification of the associated information and controlled accordingly, with particular attention to terminal entry, terminal display, and recording.

   - Controlled so that all persons to whom they have been disclosed are known to the owner or administrator.

   - Administered so that the owner or administrator is notified in event of known or suspected compromise of the passwords.

C. TERMINALS

Terminal users are responsible for ensuring that:

1. Terminals are connected to District computers only for the purpose of conducting internal business and are under District control or are in compliance with the control requirements of terminals not under District control;

2. Terminals, while unattended, are protected from unauthorized use;

3. Dial terminals, while connected, are attended or otherwise protected;

4. Permanently connected terminals, while logged on, are attended or otherwise protected;

5. Telephone numbers for computer dial ports are not posted for general view.

V. ROLE OF THE I.G. EDP AUDITOR

A. GENERAL REQUIREMENTS

The EDP Auditor conducts audits and reviews of data processing applications, installations, and organizations both to test the quality of and encourage the development of: Adequate controls and safeguarding of EDP resources, the effective utilization of data processing resources, and the adherence to management policies. The general requirements for the EDP Auditor are:

- Determining the adequacy and effective application of existing data processing operations, policies, procedures, and controls;
- Promoting operational efficiency and effective control at reasonable cost;
- Determining how well the data processing assets are both accounted for and safeguarded from losses of all kinds;
- Providing an appraisal of the accuracy, completeness and reliability of data processing accounting records and internally produced reports used by management, shareholders, and other regulatory authorities;
- Providing management with recommendations for operating improvements identified or observed during the conduct of these audits;
- Promoting the development of data processing management responsibility, accountability and self-review concepts throughout the company.

Consistent with sound auditing policy, EDP audit is committed to the disciplines of independence and objectivity. This precludes audit for designing the controls, but when a particular weakness is specified the audit normally recommends an approach to follow. It should be understood that the auditor's review does not in any way relieve other persons in the organization of the responsibilities assigned to them.